Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of the claims in the application.

Listing of the Claims:

1. (Currently amended) A method of operating a storage device, comprising:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state; and
resetting ~~setting~~ the count to a base level in response to returning the storage device to an operational state.

2. (Original) The method of Claim 1, wherein the storage device is a hard disk drive.

3. (Original) The method of Claim 1, further comprising reconstructing data stored on the storage device in a restoration storage device.

4. (Original) The method of Claim 3, further comprising providing a storage device array containing said restoration storage device and said storage device.

5. (Cancelled)

6. (Previously presented) The method of Claim 1, wherein said returning the storage device from the forced failure state to an operational state comprises reformatting the storage device.

7. (Previously presented) A method of operating a storage device, comprising:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state, wherein said returning the storage device from the forced failure state to an operational state comprises decreasing the threshold limit for the storage device after placing the storage device into a forced failure state; and
setting the count to a base level.

8. (Previously presented) A method of operating a storage device, comprising:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state, wherein said returning the storage device from the forced failure state to an operational state comprises increasing the base level after placing the storage device into a forced failure state; and
setting the count to a base level.

9. (Original) The method of Claim 1, wherein said detecting data integrity errors in the storage device comprises:
retrieving data from the storage device;
comparing the retrieved data to redundancy data; and
indicating a data integrity error if the retrieved data does not correspond with the redundancy data.

10. (Original) The method of Claim 9, wherein said redundancy data is checksum

data.

11. (Original) The method of Claim 9, wherein said retrieving data from the storage device is performed on a predetermined read schedule.

12. (Original) The method of Claim 11, wherein:
said retrieving data from the storage device comprises retrieving all of the data stored on the storage device; and
said comparing the retrieved data to redundancy data comprises comparing all of the data stored on the storage device to redundancy data.

13. (Currently amended) ~~The method of Claim 1, further comprising:~~
A method of operating a storage device, comprising:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state,
tracking the time elapsed after a first data integrity error; ~~and~~
decreasing the count if the time elapsed after the first data integrity error and before a second data integrity error is greater than a preset refresh period; and
setting the count to a base level.

14. (Original) The method of Claim 1, further comprising: storing the count on the storage device.

15. (Currently amended) A storage system, comprising:
a storage device; and
a demerit monitor coupled to the storage device operable to:
detect data integrity errors in the storage device;

count each data integrity error in a count;

when the count reaches a threshold limit, place the storage device into a forced failure state;

return the storage device from the forced failure state to an operational state; and

reset ~~set~~ the count to a base level in response to returning the storage device to an operational state.

16. (Original) The storage system of Claim 15, wherein the storage device is a hard disk drive.

17. (Previously presented) The storage system of Claim 15, further comprising a storage device controller, wherein said storage device controller includes said demerit monitor.

18. (Original) The storage system of Claim 15, further comprising an array controller, wherein said array controller includes said demerit monitor.

19. (Original) The storage system of Claim 15, further comprising:

a storage controller coupled to a plurality of storage devices;

wherein said demerit monitor is provided in the storage controller and is coupled to each of the plurality of storage devices for detecting data integrity errors in each of the plurality of storage devices, counting each data integrity error for each of the plurality of storage devices in a count, and when the count for one of the plurality of storage devices reaches a threshold limit, placing the one storage device into a forced failure state.

20. (Original) The storage system of Claim 19, further comprising:

a count table maintaining the count for each of the plurality of storage devices.

21. (Cancelled)

22. (Original) The storage system of Claim ~~21~~ 16, wherein said demerit monitor reconstructs data stored on the storage device in a restoration storage device and reformats the storage device.

23. (Previously presented) A storage system, comprising:
a storage device; and
a demerit monitor coupled to the storage device operable to:
detect data integrity errors in the storage device;
count each data integrity error in a count;
when the count reaches a threshold limit, place the storage device into a forced failure state, wherein said demerit monitor decreases the threshold limit for the storage device after placing the storage device into a forced failure state;
return the storage device from the forced failure state to an operational state; and
set the count to a base level.

24. (Previously presented) A storage system, comprising:
a storage device; and
a demerit monitor coupled to the storage device operable to:
detect data integrity errors in the storage device;
count each data integrity error in a count;
when the count reaches a threshold limit, place the storage device into a forced failure state, wherein said demerit monitor increases the base level after placing the storage device into a forced failure state;
return the storage device from the forced failure state to an operational state; and
set the count to a base level.

25. (Original) The storage system of Claim 15, wherein said demerit monitor retrieves data from the storage device, compares the retrieved data to redundancy data, and indicates a data integrity error if the retrieved data does not correspond with the redundancy data.

26. (Original) The storage system of Claim 25, wherein the redundancy data is checksum data.

27. (Original) The storage system of Claim 25, wherein said demerit monitor retrieves data from the storage device on a predetermined read schedule.

28. (Previously presented) The storage system of Claim 27, wherein said demerit monitor retrieves all of the data stored on the storage device, and compares all of the data stored on the storage device to redundancy data.

29. (Currently amended) ~~The storage system of Claim 15, wherein said demerit monitor tracks the time elapsed after a first data integrity error, and decreases the count if the time elapsed after the first data integrity error and before a second data integrity error is greater than a refresh period.~~

A storage system, comprising:

a storage device; and

a demerit monitor coupled to the storage device operable to:

detect data integrity errors in the storage device;

count each data integrity error in a count;

track the time elapsed after a first data integrity error; and

decrease the count if the time elapsed after the first data integrity error and before a second data integrity error is greater than a refresh period;

when the count reaches a threshold limit, place the storage device into a forced failure state, return the storage device from the forced failure state to an operational state; and

set the count to a base level.

30. (Previously presented) The storage system of Claim 15, wherein said count is stored on the storage device.

31. (Previously presented) A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state; and
resetting ~~setting~~ the count to a base level in response to returning the storage device to an operational state.

32. (Original) The computer-readable medium of Claim 31, wherein the storage device is a hard disk drive.

33. (Original) The computer-readable medium of Claim 31, wherein the steps further comprise reconstructing data stored on the storage device in a restoration storage device.

34. (Original) The computer-readable medium of Claim 33, wherein the steps further comprise
providing a storage device array containing said restoration storage device and said storage device.

35. (Cancelled)

36. (Previously presented) The computer-readable medium of Claim 31, wherein said returning the storage device from the forced failure state to an operational state comprises reformatting the storage device.

37. (Previously presented) A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state, wherein said returning the storage device from the forced failure state to an operational state comprises decreasing the threshold limit for the storage device after placing the storage device into a forced failure state; and
setting the count to a base level.

38. (Previously presented) A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state, wherein said returning the storage device from the forced failure state to an operational state comprises increasing the base level after placing the storage device into a forced failure state; and
setting the count to a base level.

39. (Original) The computer-readable medium of Claim 31, wherein said detecting data integrity errors in the storage device comprises:

retrieving data from the storage device;

comparing the retrieved data to redundancy data; and

indicating a data integrity error if the retrieved data does not correspond with the redundancy data.

40. (Original) The computer-readable medium of Claim 39, wherein said redundancy data is checksum data.

41. (Original) The computer-readable medium of Claim 39, wherein said retrieving data from the storage device is performed on a predetermined read schedule.

42. (Original) The computer-readable medium of Claim 41, wherein the steps further comprise:

said retrieving data from the storage device comprises retrieving all of the data stored on the storage device; and

said comparing the retrieved data to redundancy data comprises comparing all of the data stored on the storage device to redundancy data.

43. (Currently amended) ~~The computer-readable medium of Claim 31, wherein the steps further comprise:~~

A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:

detecting data integrity errors in the storage device;

counting each data integrity error in a count;

when the count reaches a threshold limit, placing the storage device into a forced failure state;

returning the storage device from the forced failure state to an operational state;

tracking the time elapsed after a first data integrity error; ~~and~~

decreasing the count if the time elapsed after the first data integrity error and before a second data integrity error is greater than a preset refresh period; and

setting the count to a base level.

44. (Original) The computer-readable medium of Claim 31, wherein the steps further comprise: storing the count on the storage device.